UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/459,287	12/17/1999	KOICHI KAMIJO	JA9-98-173	9962

7590 11/19/2004

WILLIAM A KINNAMAN JR.
INTELLECTUAL PROPERTY LAW
2455 SOUTH ROAD, P386
POUGHKEEPSIE, NY 12601

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/459,287
Filing Date: December 17, 1999
Appellant(s): KAMIJO ET AL.

William A. Kinnaman Jr.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 23, 2004.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

The rejection of the group consisting of claims 1-3, 5, 8 & 10-22 stand or fall together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. For the same reason, claim 4 stands or falls by itself. See 37 CFR 1.192(c)(7).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

6510520	STEINBERG
5,949,877	TRAW ET AL.
5,465,300	ALTSCHULER ET AL.

Schneier, Bruce, Applied Cryptography, Second Edition, 1996 John Wiley & Sons, p. 455.

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5, 8, 10-12, 14-19 & 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,510,520 to Steinberg in view of U.S. Patent 5,949,877 to Traw et al. (Traw). Regarding claim 1, Steinberg discloses writing digital data/file (Fig. 2 #58) from an input device/digital camera (Fig. 2 #58) to a memory device/secure storage device (Fig. 2 #60) and transferring digital data from the memory device/secure storage device (Fig. 2 #60) to a receiving device/computer (Fig. 2 #64). Steinberg discloses the need for authentication of transferred data (col. 2, lines 1-5), but does not disclose a first and second device authentication between the input device and memory device and between the memory device and receiving device. However, Traw teaches that copying and/or other misuse of data being transferred can be prevented by performing a first device authentication between a content source and a content sink (see col. 1, lines 40-49, col. 2, lines 61-65 & col. 9, lines 30-38). Public/private key pairs are assigned to compliant systems (col. 5, lines 55-67) for authentication/verification (col. 6, lines 58-67 & col. 7, lines 1-35). Traw's system also uses Diffie-Hellman key exchange/exchange of authentication value generated independently of the digital data (see col. 7, lines 36-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to perform both a first device authentication between the input device/first content source and memory device/first content sink and a second device authentication between the memory device/second content source and receiving device/second content sink to prevent copying and/or misuse of the data during transfer. One of ordinary skill in the art would have been motivated to perform such a modification to prevent copying and/or misuse of the data during transfer, as taught by Traw (col. 1, lines 40-49, col. 2, lines 61-65 & col. 9, lines 30-38). Some misuses are shown at col. 1, lines 15-36 of Steinberg.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Steinberg in view of Traw, in further view of U.S. Patent 5,465,300 to Altschuler et al. (Altschuler). Steinberg discloses a system, as modified above, but lacks determining whether to use secure or plaintext communication. Altschuler discloses a method whereby a plaintext communication is initiated between two devices/terminals (Fig. 5). Upon connection, the devices determine if a secure communication can be opened and initiate a secure mode if a secure session is possible (Fig. 5), to alleviate the need for human decision on whether or not to go secure (col. 1, lines 39-53). If the required secure signals are not received, the system works in plain-text mode (col. 6, lines 19-27), the information not being encrypted with the cryptographic keys (col. 7, lines 18-22). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify the Steinberg invention to include a means for automatically determining whether or not to use secure communication methods. One of ordinary skill in the art would have been motivated to perform such a modification to eliminate the need for human decision, as taught by Altschuler (see Fig. 5 & col. 1, lines 39-53).

Claims 13, 20 & 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Steinberg in view of Traw, as applied to claims 1, 15 & 21 above, in further view of Applied Cryptography, Second Edition by Schneier. The application of Schneier to claims 13, 20 and 22 is not being challenged in this appeal (see page 6, ¶1 of the Appeal Brief). These claims stand or fall with claim 1.

(11) Response to Argument

Applicant's arguments (Appeal Brief, page 6, ¶3 & page 7, ¶2 – page 8, ¶5) do not address the claim language, but only the security concepts the invention intends to bring about, such as data integrity and authenticated data transfers (page 7, ¶4) and the differences in the use of the instant invention and the inventions disclosed in the art of record. Applicant cannot rely on unclaimed features disclosed in the specification; the claims use the term "device authentication", which is taught in the prior art.

The following security principles are defined in Applied Cryptography, Second Edition by Bruce Schneier:

-- **Authentication**. It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else.

-- **Integrity**. It should be possible for the receiver of a message to verify that it has not been modified in transit; an intruder should not be able to substitute a false message for a legitimate one." – page 2, §*Authentication, Integrity, and Nonrepudiation*.

The following definition is taken from The American Heritage College Dictionary, Fourth Edition:

"privacy: The quality or condition of being secluded from the presence or view of others; the state of being free from unsanctioned intrusion; the state of being concealed; secrecy."

Specific responses to Applicant's arguments in Appeal Brief:

Page 6, ¶3 – Applicant argues that the instant invention is not concerned with "copying and/or other misuse" and therefore the Traw reference cannot be used. Further, applicant states that the instant invention is concerned with authenticating the data and protecting it against alteration.

Traw uses device authentication to prevent misuse of data. The authentication process renders the devices able to establish encrypted communications that use symmetric keys (col. 3, lines 45-50). Using a symmetric key, (defined as a key shared by the parties of a secret communication, but by no others), the data is secured against alteration and is authenticated. This is possible because (1) the data must come from a valid source, because it is encrypted with the key shared only by the source and the sink and (2) by encrypting the data, any modification is detectable because the data cannot be decrypted using the shared key. These are well-known principles of symmetric key cryptography. Further, Traw teaches "device authentication which excludes the use of devices which can circumvent the protection of the content" (col. 11, lines 37-39). This is the same advantage sought by applicant in limiting a "data transfer route to the receiving device via the memory from the input device of the digital data" (Specification, p. 2, last ¶). Therefore, the Traw reference is a valuable teaching as to the benefits of device authentication in a system where data authentication and integrity is of concern.

Page 6, ¶4 – Applicant states that "the data transfer is either ordinary or authenticated, with an authentication flag being set to mark the difference (page 5, lines 19-22), depending on the result of device authentication (page 5, steps 1.1-1.2 and 1.5)."

Applicant is reminded that the setting of an authentication flag is not recited in the claims and the term authenticated data cannot be defined so narrowly (see Schneier's definition above).

Page 7, ¶4 – Applicant argues that Altschuler is concerned with privacy (plaintext versus encrypted) and that the instant invention is concerned with integrity (authenticated versus unauthenticated data).

Page 7, ¶5 – Applicant further states that authenticated data has "originated from a definite source" and has "not been altered in the course of its transmission and storage" and argues that encrypted data is not necessarily authentic.

However, Altschuler uses cryptographic keys to exchange data (col. 7, lines 17-22). The data, encrypted by a sender, would be unreadable by a receiver if modified, because it has been encrypted with a symmetric key; the decryption process would yield unknown, unintelligible data, alerting the receiver that is has been modified. Therefore, there is a correlation between the privacy afforded by symmetric encryption and the source authentication and data integrity sought by the instant invention.

Page 8, ¶3 – Applicant argues that Altschuler "always transitions from an insecure mode of communication to a secure mode of communication, so that at the end of the secure call setup procedure, the parties are communicating either securely (if the setup procedure succeeded) or not at all (if the setup procedure failed)."

However, applicant is directed to col. 6, lines 20-27 where Altschuler state that if the secure mode command signal detection fails, a plaintext communication session continues. Thus, Altschuler's system simplifies a human-initiated secure session by automatically determining if a secure session can occur and arranging for that session if it can, so that whenever a secure session is possible, it is done. It is this teaching that is relied upon by the Examiner.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Michael J. Simitoski

Michael J. Simitoski

MJS
November 12, 2004

Conferees
Gregory Morse
Gilberto Barron, SPE 2132 GB

WILLIAM A KINNAMAN JR.
INTELLECTUAL PROPERTY LAW
2455 SOUTH ROAD, P386
POUGHKEEPSIE, NY 12601

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100